SLACKATHON PROJECT

FRAUD DETECTION

CONTENTS :

SHORT DESCRIPTION :

What's the problem?

Fraud detection is a set of activities undertaken to prevent money or property from being obtained through false pretenses.

Fraud detection is applied to many industries such as banking or insurance. In banking, fraud may include forging checks or using stolen credit cards. Other forms of fraud may involve exaggerating losses or causing an accident with the sole intent for the payout.

How Can Technology Help?

With Machine Learning Algorithms we analyze the patterns in attributes like locations/Ip address/accounts of known fraudsters to create a set of identifying rules that our system follows. Using these rules we can identify if the transaction is High-risk or not.

The Idea

Fraud is typically involves multiple repeated methods, making searching for patterns a general focus for fraud detection. For example, data analysts can prevent insurance fraud by making algorithms to detect patterns and anomalies

LONG DESCRIPTION

With an unlimited and rising number of ways someone can commit fraud, detection can be difficult. Activities such as reorganization, downsizing, moving to new information systems or encountering a cybersecurity breach could weaken an organization's ability to detect fraud. Techniques such as real-time monitoring for fraud is recommended. Organizations should look for fraud in financial transactions, locations, devices used, initiated sessions and authentication systems.

Fraud detection techniques

Fraud detection can be separated by the use of statistical data analysis techniques or artificial intelligence (AI).

Statistical data analysis techniques include:

- calculating statistical parameters

- regression analysis
- probability distributions and models
- data matching

AI techniques used to detect fraud include:

- Data mining classifies, groups and segments data to search through millions of transactions to find patterns and detect fraud.
- Neural networks learn suspicious-looking patterns and use those patterns to detect them further.
- Machine learning automatically identifies characteristics found in fraud.
- Pattern recognition detects classes, clusters and patterns of suspicious behavior.

Types of fraud

Fraud can be committed in different ways and different settings. For example, fraud can be committed in banking, insurance, government and healthcare sectors.

A common type of banking fraud is customer account takeover. This is when someone illegally gains access to a victim's bank account using bots. Other examples of fraud in banking include the use of malicious applications, the use of false identities, money laundering, credit card fraud and mobile fraud.

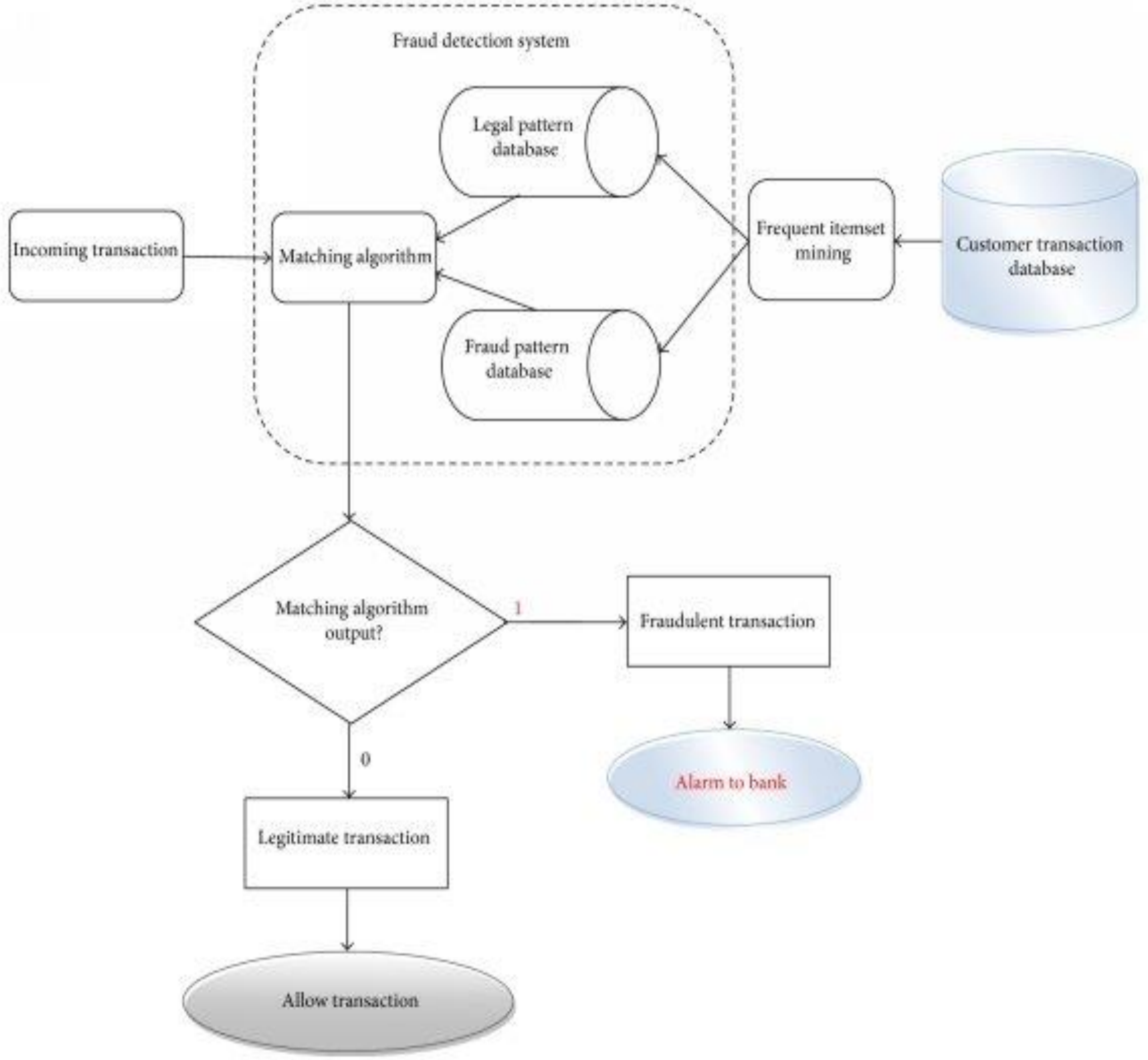
Insurance fraud includes premium diversion fraud, which is the embezzlement of insurance premiums, or free churning, which is excessive trading by a stockbroker to maximize commissions. Other forms of insurance fraud include asset diversion, workers' compensation fraud, car accident fraud, stolen or damaged car fraud, and house fire fraud. The motive behind all insurance fraud is financial profits.

Government fraud is committing fraud against federal agencies such as the U.S. Department of Health and Human Services, Department of Transportation, Department of Education or Department of Energy. Types of government fraud include billing for unnecessary procedures, overcharging for items that cost less, providing old equipment when billing for new equipment and reporting hours worked for a worker that does not exist.

Healthcare fraud includes drug fraud and medical fraud, as well as insurance fraud. Healthcare fraud is committed when someone defrauds an insurer or government health care program.

NEXT PAGE

THE ARCHITECTURE


Fraud detection system
Legal pattern database
Incoming transaction
Matching algorithm
Frequent itemset mining
Customer transaction database
Fraud pattern database
Matching algorithm output?
1
Fraudulent transaction
0
Alarm to bank
Legitimate transaction
Allow transaction